PATENT
Docket No. VIV/0015.00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gene Linetsky	Examiner: Doan, Trang
Serial No.: 10/707,602	Art Unit: 2131
Filed: December 23, 2003	APPEAL BRIEF
For: Security System with Methodology for Defending Against Security Breaches of Peripheral Devices	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

BRIEF ON BEHALF OF GENE LINETSKY

This is an appeal from the Final Rejection mailed October 15, 2007, in which currently-pending claims 1-58 stand finally rejected. Appellant filed a Notice of Appeal on January 17, 2008. This brief is submitted electronically in support of Appellant's appeal.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is assignee Check Point Software Technologies, Inc. located at 800 Bridge Parkway, Redwood City, CA 94065.

2. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellant, the Appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

The status of all claims in the proceeding is as follows:

Rejected: Claims 1-58

Allowed or Confirmed: None

Withdrawn: None

Objected to: None

Canceled: None

Identification of claims that are being appealed: Claims 1-58

An appendix setting forth the claims involved in the appeal is included as the last section of this brief.

4. STATUS OF AMENDMENTS

Two Amendments have been filed in this case. Appellant filed an Amendment on July 24, 2007, in response to a non-final Office Action dated April 24, 2007. In the Amendment, the pending claims were amended in a manner which Appellant believes clearly distinguished the claimed invention over the art of record, for overcoming the art rejections. In response to the Examiner's Final Rejection dated October 15, 2007, Appellant filed a Notice of Appeal. Subsequently, Appellant filed an Amendment After Final on March 12, 2008, for purposes of correcting minor editing informalities. In a telephone conversation with the Examiner, the undersigned confirmed that that amendment would be entered. Appellant has chosen to forgo filing any other Amendments which might further limit Appellant's claims, as it is believed that further amendments to the claims are not warranted in view of the art. Accordingly, no other

Amendments have been entered in this case after the date of the Final Rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Appellant asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 1**: a method for protecting a computer from security breaches involving devices that may be attached to the computer (see, e.g., Appellant's Specification generally at [0059]-[0070] and Fig. 4, and at [0071]-[0076] and Figs. 5A-B), where the method comprises steps of: when a device is first attached to the computer, requiring user-provided information for authorizing the device (see, e.g., Appellant's Specification at [0071]-[0072] and Fig. 5A, at 505; see also description of input filter 320 at [0055] and shown at Fig. 3); based on the user-provided information, storing authorization information indicating whether or not that the device is allowed to communicate with the computer (see, e.g., Appellant's Specification at [0073]-[0076] and at Fig. 5B, at 506-509; see also description of input filter 320 at [0055] and shown at Fig. 3); detecting detachment of the device from the computer (see, e.g., Appellant's Specification at [0071]- [0072] and at Fig. 5A, at 501-503); updating the authorization information to indicate that the device is no longer authorized to communicate with the computer (see, e.g., Appellant's Specification at [0071]- [0072] and at Fig. 5A at 504); and upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device (see, e.g., Appellant's Specification at [0071]- [0072] and at Fig. 5A at 505; and see Fig. 5B regarding untrusted status illustrated at 507 and denied/blocking illustrated at 509).

Appellant asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 23:** a system for protecting a computer from security breaches involving devices that may be attached to the computer that comprises: an agent module for specifying, in response to user-provided information, authorization information indicating whether or not a device is allowed to communicate with the computer when the device is first attached to the computer; for

detecting detachment of the device from the computer; and for updating the authorization information to indicate that the device is no longer authorized to communicate with the computer (see, e.g., Appellant's Specification at agent 330 (Fig. 3) and description at [0054]- [0055], and additionally the operation description at [0060]-[0070]; disconnection/detachment and then reconnection is described in particular detail at [0071]- [0076] and flowchart 500 in Fig. 5A-B); and a filter module for blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device (see, e.g., Appellant's Specification at input filtering module 320 (Fig. 3) and description at [0054]- [0056]).

Appellant asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 43:** a method for securing a computer from security breaches involving peripheral devices, where the method comprises steps of: specifying a password to be supplied by a user for authorizing a peripheral device to communicate with the computer (see, e.g., Appellant's Specification at [0045]- [0049]; see also Device authorization at [0050]- [0053]); detecting each attachment of the peripheral device to the computer (see, e.g., Appellant's Specification at [0071]- [0076] and flowchart 500 in Fig. 5A-B, where disconnection/detachment and then reconnection is described in particular detail); upon each attachment, blocking communications with the peripheral device until the password is supplied again by the user (see, e.g., Appellant's Specification at [0055]; see also [0073]- [0076]); and if the password is supplied, permitting the peripheral device to communicate with the computer (see, e.g., Appellant's Specification at [0076]).

6. GROUNDS OF REJECTION TO BE REVIEWED

The (sole) grounds presented on appeal are:

(1st) Whether claims 1-58 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Heinrich et al. (Pub. No. 2002/0194486) (hereinafter "Heinrich").

7. ARGUMENT

A. First Ground: Claims 1-58 rejected under Section 102

1. General

Under Section 102, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, the reference fails to teach each and every element set forth in Appellant's independent claims, as well as other claims, and therefore fails to establish anticipation of the claimed invention under Section 102.

2. Claims 1-58

Claims 1-58 stand rejected under 35 U.S.C. 102(e) as being anticipated by Heinrich et al. (Pub. No. 2002/0194486) ("Heinrich"). Here, the Examiner likens Appellant's invention to a security system for securing certain Plug and Play peripheral devices connected to an ISA (i.e., PC internal) bus. The Examiner's rejection of claims 1, 23, and 43 is representative:

> Regarding claims 1, 23 and 43, Heinrich discloses when a device is first attached to the computer, specifying authorization information indicating that the device is allowed to communicate with the computer (Heinrich: paragraphs [0009, 0021]); detecting detachment of the device from the computer (Heinrich: see Abstract section); updating the authorization information to indicate that the device is no longer authorized to communicate with the computer (Heinrich: paragraphs [0016-0017 and 0045]); and upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device (Heinrich: paragraphs [0009, 0015 and 0034-0035], the device remains locked until the passwords match).

For the reasons set forth below, Appellant's claimed invention may be distinguished on a

variety of grounds.

Heinrich describes a security system for Plug and Play peripheral devices that is internal to the computer system (i.e., it does not involve devices that users typically attach, detach, and reattach), especially when used in the context of connecting devices to an ISA bus (e.g., inserting a video card into the internal bus slot on a PC). Of particular interest to Heinrich is that those peripheral devices may contain sensitive information or passwords. Therefore, Heinrich approach is to protect those peripheral devices from security breaches (i.e., coming from the computer).

Heinrich is essentially the opposite scenario that is addressed by Appellant's invention. The problem addressed by Appellant's invention is that "bad" (untrustworthy) devices may be plugged into a computer. A "bad" peripheral device for example would include a keyboard having an in-line (e.g., dongle) key logger. In that case, the keyboard is untrustworthy (since it may steal user-provided information) and, therefore, it should be blocked (i.e., denied access) from communicating with the computer. In Heinrich's scenario, on the other hand, the peripheral devices themselves are secured (i.e., they contain sensitive information, and thus are required to be secured against unauthorized access). In that scenario, the peripheral devices themselves are not bad, but instead they are "good" devices having valuable information that should be protected from unauthorized access.

Recognizing that (when broadly interpreted) Appellant's claims could be construed to read on Heinrich's fundamentally different system, Appellant's independent claims were amended in a previously-filed amendment to highlight the above-mentioned distinctions. An important distinction is that Appellant's approach requires the user to authorize the particular peripheral device each and every time it is attached or reattached, **regardless** of whether the device is attached to the same port or slots (or otherwise assigned the same base address) as before. Here, user inspection is desirable to determine if a peripheral device has been tampered with. In Heinrich's approach, on the other hand, an internal hardware system operates to keep track of identifying information of a Plug and Play device inserted into a slot connected to the ISA bus (i.e., internal computer bus), and then potentially moved to another slot. Essentially, Heinrich is a housekeeping or accounting approach to track the movement of known "good" peripheral devices and

cards (e.g., when moved from one slot to another). Importantly, Heinrich cannot detect tampering of peripheral devices in the manner of Appellant's claimed invention, as Heinrich has no facility to detect attachment events themselves (i.e., initial attachment, detachment, and reattachment) for peripheral devices. Instead, Heinrich can only detect the changing of a base address for a device, for example as a result of moving a device from one physical slot to another physical slot.

What Heinrich really teaches is a technique for locking or binding devices (e.g., plug-in cards) to particular slots (e.g., ISA or PCI slot) of a computer. Once the device is plugged into a slot, its base address (at that slot) can be stored along with password information so that that device is "secured" to that address (slot). If someone attempts to move the device to another slot and therefore modify the base address, the Heinrich's system intervenes to prevent access to that device unless an appropriate password is entered. Note in particular that Heinrich **does not cover the scenario** where the device is removed, tampered with, and then plug it back into the same slot/same base address. This last scenario is the very specific problem (i.e., monitoring the detachment and reattachment of a device to the very same port or slot) that is addressed by Appellant's invention, and which is left completely unaddressed by Heinrich. Significantly, the biggest threat addressed by Appellant's invention -- the tampering of a keyboard -- is a threat that would not be caught at all by Heinrich, as the detachment, tampering, and reattachment of the keyboard would not yield a base address change that would allow Heinrich to detect it. The detachment, tampering, and reattachment of the keyboard are all activities that would go undetected by Heinrich.

Moreover, as Appellant pointed out in the last filed response, Heinrich really includes no provision whatsoever where his system prompts for user authorization before a device is even allowed to interact with the computer in the first place. In other words, Appellant's claimed invention operates to **completely refuse** to allow a device that it does not know about to interact with the computer at all. The device is shut down from the "get go": as soon as it is attached or reattached all communication is blocked until such time (if any) that the user authorizes the device. Heinrich provides no such feature. For example, if a hacker or disgruntled employee decided to plug a "bad" card (e.g., containing malicious software) into a computer relying solely on Heinrich's system, that

computer has no mechanism to refuse the device (i.e., prevent or shut down its operation or interaction with the operating system). Instead in Heinrich's case, such a malicious device could take over control of the computer system since its initial interaction with the computer system is not blocked by Heinrich's approach. That Heinrich's approach may later allow this malicious card to be "secured" to a particular base address or slot is irrelevant. The damage will have already been done, as the malicious card will have already gained access and control over the computer system.

In Appellant's last filed response, the independent claims were amended to emphasize that any device attachable to the computer is deemed at the outset to be untrustworthy, until such time (if any) that trust is established by the user (i.e., authorized by the user or the system administrator). For example claim 1 includes:

> **when** a device is **first attached** to the computer, requiring user-provided information for authorizing the device;
>
> (Emphasis added.)

Here, the claim makes it clear that Appellant's claimed approach basically assumes any attached device is un-trusted until proven otherwise. This "trust no one" or "trust no device" strategy is only provided by Appellant's invention; it is not provided by Heinrich.

A device becomes trusted only when a user (with appropriate privileges) indicates that he or she now vouches for the device (e.g., by entering information indicating that the device is authorized for attachment to the computer, for example after appropriate visual inspection of the device). The user himself or herself may be located at the machine, or may be located remotely (e.g., remote administrator). If the device is not authorized by the user, then the device retains its un-trusted status, whereupon communication of the un-trusted device with the computer is blocked. For example in the case of a "bad" keyboard, the keyboard would be completely blocked from communicating with the computer at the outset (i.e., it would not work). Importantly in this scenario, when a trusted device becomes unplugged and then is later reattached, Appellant's approach is to again treat it as an un-trusted device again until such time that

it can be re-authenticated by the user (and irrespective of whether or not any base address for the device has changed).

In the Examiner's Final Rejection, the Examiner sets up a "straw man" argument based on the notion that Appellant argued that Heinrich provided no user interaction (e.g., user-entered passwords). Appellant does not argue that Heinrich is without user interaction, as it obviously involves user interaction for securing or binding peripheral devices to a given slot or base address. What Appellant argued -- and what Appellant again asserts to be the case -- is that Heinrich contains no teaching or suggestion that a given device be authorized by a user at the very outset when it is first attached (i.e., **before** it is allowed to interact with the computer system). As described above, Heinrich clearly operates after the fact (i.e., after the physical install of the device). Heinrich has no preemptive ability to block devices. It only has the ability to catch a previously installed device moving from one slot (base address) to another, which is the technique it uses to secure a device to a given slot. Moreover, Heinrich contains no teaching or suggestion that a given device be **reauthorized** by a user **at each and every subsequent reattachment event** (i.e., regardless of whether the base address for the device has changed).

In view of the foregoing distinguishing features (as well as Appellant's previously-filed clarifying amendments to the independent claims), it is respectfully submitted that Appellant's invention provides an important and patentable advance over the art, one that is not taught or suggested by the art of record. Using Appellant's invention, for example, it is now possible to detect malicious tampering of a detachable keyboard device. If a hacker or malicious individual attempted to unplug a keyboard at a public Internet café for purposes of inserting a key logger dongle, for example, Appellant's invention would catch that event and would refuse to reauthorize the keyboard, until such time as an appropriately authorized individual (e.g., Internet café employee or system administrator) came along, inspected the keyboard for tampering, and then reauthorized the keyboard (if observed to be untampered). Applying the teachings of Heinrich to this scenario simply does not work. Heinrich clearly has no mechanism described that detects attempts to tamper peripheral devices based on mere attachment or reattachment events (i.e., without regard to what slot or port they are

plugged into). And Heinrich certainly has no mechanism where it refuses the initial attachment of an unknown peripheral devices or it refuses reattachment of a known peripheral device to the same slot or port (until that reattachment is authorized). The previously-amended claims are believed to distinguish over the cited art. Accordingly, it is respectfully requested that the Examiner's rejection under Section 102 not be sustained.

B. Conclusion

The present invention greatly improves the ease and efficiency of the task of protecting a computer from security breaches involving devices that may be attached, detached, and reattached to the computer. The cited Heinrich reference does not provide this capability. It is respectfully submitted that the present invention, as set forth in the pending claims, sets forth a patentable advance over the art.

In view of the above, it is respectfully submitted that the Examiner's rejections under 35 U.S.C. Section 102 should not be sustained. If needed, Appellant's undersigned attorney can be reached at 408 884 1507. For the fee due for this Appeal Brief, please refer to the attached Fee Transmittal Sheet. This Brief is submitted electronically.

Respectfully submitted,

Date: March 31, 2008

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX

8. CLAIMS APPENDIX

1. A method for protecting a computer from security breaches involving devices that may be attached to the computer, the method comprising:

when a device is first attached to the computer, requiring user-provided information for authorizing the device;

based on the user-provided information, storing authorization information indicating whether or not that the device is allowed to communicate with the computer;

detecting detachment of the device from the computer;

updating the authorization information to indicate that the device is no longer authorized to communicate with the computer; and

upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

2. The method of claim 1, wherein said storing step includes:

specifying a password for authorizing the device.

3. The method of claim 1, wherein said storing step includes:

specifying at least one user with sufficient privileges to authorize the device.

4. The method of claim 1, wherein the device is attached to the computer via a port.

5. The method of claim 4, wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port.

6. The method of claim 1, wherein said device comprises an input device and wherein said blocking step includes blocking input from the input device.

7. The method of claim 6, wherein said input device is a keyboard device.

8. The method of claim 7, further comprising:

upon reattachment of the keyboard device, trapping keystrokes from the keyboard device.

9. The method of claim 8, further comprising:

determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

10. The method of claim 1, wherein said device comprises a detachable storage device and wherein said blocking step includes blocking any data stream from the storage device.

11. The method of claim 1, wherein said blocking step includes:

blocking communication from the computer to the device while the device remains unauthorized.

12. The method of claim 1, further comprising:

receiving input authorizing the device; and thereafter

allowing communication with the device.

13. The method of claim 12, wherein the input comprises password input from an authorized user.

14. The method of claim 1, further comprising:

upon detecting detachment of the device from the computer, generating an alert that reports the detachment.

15. The method of claim 14, wherein the alert is automatically transmitted to a system administrator.

16. The method of claim 14, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

17. The method of claim 1, further comprising:

receiving authorization from a remote administration module; and thereafter allowing communication with the device.

18. The method of claim 1, wherein said storing step includes:

specifying an operating system hook that allows attachment and detachment of devices to be detected.

19. The method of claim 1, wherein said updating step includes:

updating the authorization information to indicate that the device is currently untrusted.

20. The method of claim 1, wherein said updating step includes:

treating the detachment as a security breach and blocking communication with a network node that the computer resides on.

21. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

22. A downloadable set of processor-executable instructions for performing the method of claim 1.

23. A system for protecting a computer from security breaches involving devices that may be attached to the computer, the system comprising:

an agent module for specifying, in response to user-provided information, authorization information indicating whether or not a device is allowed to communicate with the computer when the device is first attached to the computer; for detecting detachment of the device from the computer; and for updating the authorization

information to indicate that the device is no longer authorized to communicate with the computer; and

a filter module for blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

24. The system of claim 23, wherein the agent module includes:

program logic for specifying a password for authorizing the device.

25. The system of claim 23, wherein the agent module includes:

program logic for specifying at least one user with sufficient privileges to authorize the device.

26. The system of claim 23, wherein the device is attached to the computer via a port.

27. The system of claim 26, wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port.

28. The system of claim 23, wherein said device comprises an input device and wherein the filter module includes program logic for blocking input from the input device.

29. The system of claim 28, wherein said input device is a keyboard device.

30. The system of claim 29, wherein said filter module includes:

program logic for trapping keystrokes from the keyboard device.

31. The system of claim 30, wherein said filter module further includes:

program logic for determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

32. The system of claim 23, wherein said device comprises a detachable storage device and wherein the filter module includes program logic for blocking any data stream from the storage device.

33. The system of claim 23, wherein the filter module includes:

program logic for blocking communication from the computer to the device while the device remains unauthorized.

34. The system of claim 23, wherein said modules further comprise:

program logic for receiving input authorizing the device, and thereafter

program logic for allowing communication with the device.

35. The system of claim 34, wherein the input comprises password input from an authorized user.

36. The system of claim 23, wherein said agent module further comprises:

program logic for generating an alert that reports the detachment.

37. The system of claim 36, wherein the alert is automatically transmitted to a system administrator.

38. The system of claim 36, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

39. The system of claim 23, wherein said modules further comprises:

program logic for receiving receiving authorization from a remote administration module; and thereafter

program logic for allowing communication with the device.

40. The system of claim 23, wherein the agent module includes:

program logic for specifying an operating system hook that allows attachment and

detachment of devices to be detected.

41. The system of claim 23, wherein the agent module includes:

program logic for updating the authorization information to indicate that the device is currently untrusted.

42. The system of claim 23, wherein the agent module includes:

program logic for treating the detachment as a security breach and blocking communication with a network node that the computer resides on.

43. A method for securing a computer from security breaches involving peripheral devices, the method comprising:

specifying a password to be supplied by a user for authorizing a peripheral device to communicate with the computer;

detecting each attachment of the peripheral device to the computer;

upon each attachment, blocking communications with the peripheral device until the password is supplied again by the user; and

if the password is supplied, permitting the peripheral device to communicate with the computer.

44. The method of claim 43, wherein said specifying step includes:

specifying at least one user with sufficient privileges to authorize the peripheral device.

45. The method of claim 43, wherein the peripheral device is attached to the computer via a port.

46. The method of claim 43, wherein said peripheral device comprises an input device and wherein said blocking step includes blocking input from the input device.

47. The method of claim 46, wherein said input device is a keyboard device.

48. The method of claim 47, further comprising:

upon reattachment of the keyboard device, trapping keystrokes from the keyboard device.

49. The method of claim 48, further comprising:

determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

50. The method of claim 43, wherein said blocking step includes:

blocking communication from the computer to the peripheral device while the peripheral device remains unauthorized.

51. The method of claim 43, further comprising:

upon any detachment of the peripheral device from the computer, generating an alert that reports the detachment.

52. The method of claim 51, wherein the alert is automatically transmitted to a system administrator.

53. The method of claim 51, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

54. The method of claim 43, further comprising:

receiving the password from a remote administration module; and thereafter

allowing communication with the peripheral device.

55. The method of claim 43, wherein said specifying step includes:

specifying an operating system hook that allows attachment and detachment of peripheral devices to be detected.

56. The method of claim 43, further comprising:

treating any detachment of the peripheral device as a security breach and blocking communication with a network node that the computer resides on.

57. A computer-readable medium having processor-executable instructions for performing the method of claim 43.

58. A downloadable set of processor-executable instructions for performing the method of claim 43.

9. EVIDENCE APPENDIX

This Appeal Brief is not accompanied by an evidence submission under §§ 1.130, 1.131, or 1.132.

10. RELATED PROCEEDINGS APPENDIX

Pursuant to Appellant's statement under Section 2, this Appeal Brief is not accompanied by any copies of decisions.